

DOCUMENT DE
PRIORITÉ
PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA REGLE
17.1.a) OU b)

FR 00/311



PCT/FR 00/00311

REC'D 28 FEB 2000

WIPO

PCT

ETJ

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **15 FEV. 2000**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

La présente invention concerne un système de mesure des durées de transfert et des taux de perte pour des réseaux de télécommunication en mode paquet.

Les réseaux de télécommunication en mode paquet se caractérisent en ce que les informations acheminées sont véhiculées en groupes appelés paquets, essentiellement constitués d'un en-tête contenant les informations pour l'acheminement du paquet dans le réseau et des données à transmettre. Ces paquets sont véhiculés à travers le réseau, et empruntent au gré de ce réseau des moyens de transmission et de commutation les plus variés.

Un exemple de réseau en mode paquet est le réseau Internet, fonctionnant avec le protocole IP (Internet Protocol). Quelques exemples de moyens de transmission et de commutation associés au protocole IP sont des réseaux RNIS (Réseau Numérique à Intégration de Service), FR (Frame Relay), ATM (Asynchronous Transfer Mode), SDH (Synchronous Digital Hierarchy), SONET (Synchronous Optical Network), DWDM (Dense Wavelength Digital Multiplexing), etc.

Les paquets sont typiquement émis par un grand nombre de sources fonctionnant indépendamment les unes des autres, vers un grand nombre de destinations fonctionnant également indépendamment les unes des autres. Les instants d'émission des paquets ne sont pas déterminés finement par le réseau lui-même. Il en est de même pour la longueur de chaque paquet. Il est alors difficile pour l'exploitant et les utilisateurs du réseau de garantir, voire même d'estimer les caractéristiques temporelles (durée du transfert) et le taux de perte (probabilité qu'un paquet ne soit pas délivré à son destinataire). Il est donc très utile de pouvoir effectuer des mesures précises des valeurs réelles sur les paquets utiles, pour permettre l'administration, la configuration, la planification du réseau en mode paquet. Une bonne connaissance de ces caractéristiques facilite également la mise en place de

services à qualité différenciée et garantie (par opposition au service « au mieux » ou « best effort » en anglais).

Une solution classique consiste à employer une ou
5 plusieurs sources qui émettent des paquets de test (ces paquets
sont souvent appelés « ping » dans le cas de réseau IP). Chaque
paquet est reconnu par son destinataire et renvoyé par celui-ci
auprès de la source correspondante. Celle-ci peut alors
effectuer des mesures, par exemple le temps aller-retour. Il
10 est aussi possible d'effectuer des traitements statistiques à
partir des mesures faites sur un grand nombre de paquets ; par
exemple estimer les caractéristiques des durées de transfert
aller-retour (maximum, minimum, moyenne, médiane, etc.) ou
estimer des taux de perte de paquet.

15

Une autre solution utilisée consiste à pourvoir une
partie des sources et des destinataires d'une connaissance
suffisamment précise d'une référence de temps commune. Les
sources génèrent des paquets de test et notent l'heure de
20 départ. Les destinataires notent l'heure de réception de ces
paquets de test. Des calculs sont ensuite effectués pour
caractériser par exemple les durées de transfert et les taux de
perte.

25

Néanmoins ces solutions ne permettent pas d'obtenir une
bonne précision dans tous les cas. En effet, le nombre des
paquets de test doit rester petit pour ne pas trop charger le
réseau ni mobiliser trop d'équipements ; les estimations
statistiques peuvent donc être entachées d'une imprécision
30 importante. Par ailleurs, les réseaux en mode paquet n'offrent
souvent pas des caractéristiques identiques pour les chemins
aller et retour entre deux points d'accès. De plus, les
équipements de réseau en mode paquet (par exemple les routeurs
et commutateurs) effectuent souvent l'analyse du contenu du
35 paquet (par exemple le protocole de transport de bout en bout,

le type de données, le type de fichier contenu dans le paquet, etc.) pour en déduire leur méthode d'acheminement du paquet (par exemple, la file d'attente, ou la priorité, etc.) ; il n'est donc pas certain que les paquets de test empruntent le
5 même chemin que les paquets contenant les données réelles des usagers du réseau.

Le but de la présente invention est de pallier les inconvénients précités. A cet effet, l'invention a pour objet
10 un dispositif à architecture répartie permettant d'effectuer des mesures précises des durées de transfert et des taux de perte pour des réseaux de télécommunication en mode paquet. L'invention comporte des moyens de mesure (datation, classification et identification des paquets), des moyens de
15 compression des mesures, des moyens de transmission des mesures, des moyens de collecte et de corrélation, des moyens de stockage, des moyens d'analyse et des moyens d'exploitation.

L'invention a comme avantage de ne pas nécessiter
20 l'utilisation de paquets de test, ce qui permet d'atteindre une très grande représentativité de chaque mesure. Elle a également pour avantage de pouvoir effectuer un très grand nombre de mesures, ce qui permet d'offrir une très grande précision statistique. Enfin, le nombre de mesures effectuées peut être
25 modulé en fonction des types de données véhiculés dans les paquets, ce qui permet une utilisation rationnelle des ressources disponibles du système. D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit faite en regard des dessins annexés qui
30 représentent :

- La figure 1 les principaux sous-ensembles fonctionnels qui composent l'invention.

- La figure 2 un exemple de déploiement de l'invention dans un réseau de télécommunication en mode paquet.

- La figure 3 un exemple d'organisation fonctionnelle interne du sous-ensemble (1)

L'invention peut se découper en 5 principaux sous-ensembles fonctionnels, de la façon représentée à la figure 1. Un premier sous-ensemble (1) réalise les fonctions de mesure (datation, classification et identification des paquets), de compression de ces mesures et de transmission des mesures vers le deuxième sous-ensemble (2). Un deuxième sous-ensemble (2) réalise les fonction de collecte et de corrélation des mesures élémentaires effectuées par le sous-ensemble (1). Un troisième sous-ensemble (3) réalise les fonctions de stockage des mesures corrélées. Un quatrième sous-ensemble (4) réalise les fonctions d'analyse des mesures corrélées. Un cinquième sous-ensemble (5) réalise les fonctions d'exploitation associées aux résultats de l'analyse.

Ces différents sous-ensembles peuvent être physiquement dissociés, ou bien partiellement ou totalement localisés dans un ou des équipements physiques communs.

Un exemple simple de déploiement dans un réseau est représenté par la figure 2. Les usagers (6₁), (6₂) et (6₃) sont reliés à un réseau de télécommunication en mode paquet (7) (par exemple un réseau à base du protocole IP - Internet Protocol). Les sous-ensembles (1₁) et (1₄) ont accès aux paquets (8₁) émis par (6₁) ; le sous-ensemble (1₂) a accès aux paquets émis par (6₂) ; le sous-ensemble (1₃) a accès aux paquets reçus par (6₃). Le sous-ensemble (2) est relié au réseau (7) et se comporte comme un usager de ce réseau ; il communique par ce moyen avec les sous-ensembles (1₁), (1₂), (1₃) et (1₄) qui sont aussi des usagers du réseau (7). Les sous-ensembles (3), (4) et (5) ne sont pas représentés. Les sous-ensembles (1₁), (1₂),

(13) et (14) effectuent les opérations de mesure pour chacun des paquets auxquels ils ont accès (datation, classification et identification des paquets), ainsi que les fonctions de compression de ces mesures (l'ensemble de ces fonctions est décrits plus loin). Ils communiquent chacun par le réseau (7) les mesures compressées au sous-ensemble (2) qui corrèle l'ensemble de ces mesures.

D'autres configurations de déploiement sont également possibles au titre de la présente invention. Notamment les cas suivants :

- Les usagers (6) ne sont pas forcément les utilisateurs finaux des informations véhiculées dans les paquets ; ils peuvent représenter par exemple non limitatif des réseaux locaux, ou d'autres réseaux en mode paquet.

- Les sous-ensembles (1) peuvent être reliés au sous-ensemble (2) par d'autre moyens que le réseau en mode paquet (7); par exemple, au moyen d'un autre réseau de télécommunication, ou au moyen d'un support de stockage local enregistrant les données du sous-ensemble (1) et les restituant au sous-ensemble (2) ultérieurement.

- Un même sous-ensemble (1) peut être relié à plusieurs sous-ensemble (2).

- Plusieurs sous-ensembles (2) peuvent communiquer pour élaborer des corrélations entre les éléments de mesure dont ils disposent.

Une découpe fonctionnelle possible du sous-ensemble (1) est représentée à titre d'exemple à la figure 3. On y trouve quatre groupes fonctionnels :

- Le groupe des règles (10), fixées de façon statique ou semi-statique (par exemple par l'exploitant du système).

- Le groupe de l'évaluation de la charge (20), mesurant le taux de charge du CPU local, les occupations mémoires, etc.

- Le groupe de calcul (30), évaluant dynamiquement les valeurs de compactage, d'échantillonnage, etc.

- Le groupe chemin de données (40), produisant des enregistrements contenant des combinaisons (classe, date, signature) pour chacun des paquets.

Les principes généraux de la mesure par le sous-ensemble (1) sont précisés ci-après :

- Les sous-ensembles (1) possèdent un moyen d'acquérir et de maintenir une référence temporelle commune (31). L'imprécision de cette référence entre deux sous-ensembles (1) affecte directement la précision du résultat de l'ensemble du dispositif. Les moyens d'acquisitions de cette référence temporelle peuvent être divers et multiples ; citons à titre d'exemples non limitatifs le GPS (Global Positionning System), la diffusion au moyen d'ondes radio, les pilotes à haute stabilité, les protocoles NTP (Network Time Protocol) et SNTP (Simple Network Time Protocol).

- Chaque paquet fait l'objet d'une datation (41) (en utilisant la référence temporelle absolue) lors de son observation par le sous-ensemble (1). Celui-ci peut dater soit le début du paquet, soit la fin du paquet, soit tout autre critère.

- Chaque paquet fait l'objet d'un calcul de signature (42), destiné à le représenter par la suite. La signature permet de réduire le volume d'information nécessaire pour identifier le paquet. Cette signature est typiquement le résultat d'un calcul polynomial binaire (par exemple un calcul de CRC - Code de Redondance Cyclique - sur 16 ou 32 éléments binaires). Le calcul de signature est effectué sur tout le paquet ou sur une partie de celui-ci, en fonction de considérations liées à la structure et à la variabilité du contenu des paquets dans le réseau. La signature doit être petite devant la taille moyenne du paquet, pour faciliter son stockage, sa transmission et sa manipulation ultérieure. Elle

doit pouvoir prendre suffisamment de valeurs différentes pour rendre négligeable la probabilité que deux paquets aient une signature identique. A titre d'exemple, on peut considérer qu'une signature sur 16 éléments binaires permet d'identifier de l'ordre de 256 paquets différents avec une faible probabilité d'équivoque.

- Chaque paquet fait l'objet d'une opération de classification (44). Les critères de classification sont typiquement ceux classiquement retenus pour identifier des flux entre réseaux et sous-réseau (sous-adresses réseau IP, par exemple), des flux entre équipements terminaux (adresses IP, par exemple), des flux entre applications (adresses IP et adresses transport UDP/TCP, par exemple), etc. Chaque paquet est alors identifié par une combinaison de tout ou partie des éléments: classe, date, signature.

- Chaque classe peut faire l'objet de filtrage (45); c'est à dire que le sous-ensemble (1) ne mémorise pas les combinaisons (classe, date, signature) des paquets appartenant à une des classes pour lesquelles le filtre est mis en place.

- Chaque classe peut faire l'objet d'une opération d'échantillonnage semi-statique (46). Dans ce cas, seule une partie des combinaisons (classe, date, signature) des paquets appartenant à une classe donnée sera retenue. Le taux d'échantillonnage dépend typiquement de la classe, et ne varie en principe pas de façon dynamique. Par exemple, on peut vouloir conserver toutes les combinaisons pour les paquets véhiculant de la voix, et une fraction de ceux véhiculant des fichiers informatiques.

- Chaque classe peut faire l'objet d'un échantillonnage dynamique, dont le taux dépend des conditions de congestion du système: mesure de l'occupation des tampons (21) et mémoires (22) du sous-ensemble (1), débit d'émission vers le sous-ensemble (2), charge du réseau, charge du sous-ensemble (2), etc. Une multiplicité de critères peut être utilisée pour que le fonctionnement global se situe automatiquement dans la zone

la plus satisfaisante pour l'administrateur du dispositif (par exemple non limitatif, le taux d'échantillonnage le plus fort pour un débit réseau maximum donné, ou encore le débit réseau minimum pour un taux d'échantillonnage donné).

5 - On peut joindre à chaque combinaison (classe, date, signature) retenue un compteur indiquant le nombre de paquet observé dans le flux. Le sous-ensemble (2) peut alors faire une mesure du taux de perte dans le réseau en comparant les compteurs associés aux mêmes paquets aux différents points du
10 réseau.

Les opérations de filtrage et d'échantillonnage statique et dynamique permettent de réduire la quantité de combinaisons (classe, date, signature) à mémoriser et à traiter
15 .La mise en place ou le retrait des filtres, les valeurs de taux d'échantillonnage semi-statique, la politique de paramétrage de l'échantillonnage dynamique, etc., peuvent par exemple être réalisée au moyen d'une opération d'administration effectuée depuis l'un des sous-ensembles (2) ou (5).

20 Les critères d'échantillonnage peuvent être divers. A titre d'exemple non limitatif, on peut citer l'échantillonnage périodique (on garde une combinaison toutes les N combinaisons), l'échantillonnage statistique conditionné par le tirage d'une variable aléatoire dont on maîtrise les
25 caractéristiques statistiques et l'échantillonnage sur signature (on ne garde que les combinaisons dont la signature appartient à un ensemble donné de valeurs).

L'ordre dans lequel le sous-ensemble (1) effectue les opérations décrites précédemment peut varier (par exemple, le
30 sous-ensemble (1) peut classer les paquets avant d'effectuer la datation, si ça n'affecte pas trop la précision de la mesure). De même, les opérations de filtrage peuvent être effectuées à différents instants du processus, sans que cela n'en change les principes inventifs.

Les principes généraux de collecte et de corrélation des mesures par le sous-ensemble (2) sont précisés ci-après:

- Le sous-ensemble (2) reçoit les échantillons des combinaisons (classe, date, signature) non filtrées en provenance de tous les sous-ensembles (1) qui lui sont rattachés.

- Chaque paquet est en principe vu par deux sous-ensembles (1): une première fois à l'entrée dans le réseau et une deuxième à la sortie. Toutefois d'autres cas sont possibles ; par exemple un paquet peut n'être vu qu'une fois si le domaine de surveillance des sous-ensemble (1) n'est pas clos, ou plus de deux fois si il y a des sous-ensembles (1) à l'intérieur du réseau.

- Chaque observation du passage du paquet auprès d'un sous-ensemble (1) donne lieu à la réception par le sous-ensemble (2) de 1 ou 0 combinaisons (zéro si filtrage, échantillonnage, perte du message de retour, etc.).

- Le sous-ensemble (2) essaye de corréler les combinaisons (classe, date, signature) concernant un même paquet, par exemple en utilisant la comparaison des signatures et un majorant des délais de transit dans le réseau.

- En cas de succès, il en déduit par un calcul arithmétique simple d'une part le délai de transfert entre les différents sous-ensembles (1) pour le paquet considéré, et d'autre part le nombre de paquets éventuellement perdus dans le réseau. De plus, un excès de paquets en sortie peut indiquer une défaillance d'un des équipements du réseau, ou une tentative d'intrusion.

- Des calculs plus évolués (par exemple non limitatif les valeurs moyenne, minimale, maximale, médiane, etc. pour une tranche de temps et un type de flux donné) peuvent également être effectués dans le sous-ensemble (2) avant stockage par le sous-ensemble (3).

Le choix d'un ensemble de critères de filtrage et d'échantillonnage statique et dynamique cohérents pour la totalité des sous-ensembles (1) attachés à un sous-ensemble (2) facilite les opérations de corrélation effectuées par ce
5 dernier, et améliore la proportion des corrélations réussies.

Les principes de stockage du sous-ensemble (3), d'analyse du sous-ensemble (4) et d'exploitation du sous-ensemble (5) ne sont pas détaillés ici.

REVENDICATIONS

1. Dispositif à architecture distribuée pour la mesure précise et sans injection de trafic de test, des durées de transfert et des taux de perte dans les réseaux en mode paquet, par exemple les réseaux à base du protocole IP (Internet Protocol), et comprenant : une multiplicité de sous-ensembles (1) réalisant les fonctions de mesure (datation, classification et identification des paquets), de compression notamment par filtrage et échantillonnage de ces mesures et de transmission des mesures vers le deuxième sous-ensemble (2); un deuxième sous-ensemble (2) réalisant les fonctions de collecte et de corrélation des mesures élémentaires effectuées par le sous-ensemble (1) ; un troisième sous-ensemble (3) réalisant les fonctions de stockage des mesures corrélées; un quatrième sous-ensemble (4) réalisant les fonctions d'analyse des mesures corrélées, un cinquième sous-ensemble (5) réalisant les fonctions d'exploitation associées aux résultats de l'analyse.

2. Dispositif selon la revendication 1, caractérisé en ce que chaque paquet observé fait l'objet d'une datation selon une référence temporelle commune à chacun des sous-ensemble (1).

3. Dispositif selon l'une quelconque des revendications 1 et 2, caractérisé en ce que chaque paquet observé fait l'objet du calcul d'une séquence binaire courte et représentative de son contenu ; cette séquence est appelée signature.

4. Dispositif selon l'une quelconque des revendications 1, 2 et 3, caractérisé en ce que chaque paquet est classé selon ses caractéristiques de destination ou le type de son contenu.

5. Dispositif selon l'une quelconque des revendications 1, 2, 3 et 4, caractérisé par l'association à chaque paquet d'une combinaison (classe, date, signature) le représentant sous une forme compacte.

6. Dispositif selon la revendication 5, et caractérisé en ce que les combinaisons (classe, date, signature) associées à chaque paquet peuvent être éliminées sur des critères dépendants de la configuration du dispositif, de la classe à laquelle appartient le paquet concerné et d'informations sur la charge des différents sous-ensembles.

7. Dispositif selon la revendication 5, et caractérisé en ce que les combinaisons (classe, date, signature) associées à chaque paquet peuvent être sélectionnées par échantillonnage sur des critères dépendant de la configuration du dispositif, de la classe à laquelle appartient le paquet concerné et d'informations sur la charge des différents sous-ensembles.

8. Dispositif selon la revendication 5, et caractérisé en ce que un compteur de paquets est associé aux combinaisons (classe, date, signature). Ce compteur indique le nombre de paquets reçus dans la classe considérée.

9. Dispositif selon la revendication 5, et caractérisé par une opération de mise en correspondance des combinaisons (classe, date, signature) appartenant à un même paquet observé par plusieurs sous-ensembles (1). Cette mise en correspondance permet le calcul des durées de transfert dans différentes portions du réseau.

10. Dispositif selon la revendication 5 et 8, et caractérisé par une opération de mise en correspondance des combinaisons (classe, date, signature) et des compteurs des paquets appartenant à une même classe et observés par plusieurs sous-ensembles (1). Cette mise en correspondance permet le calcul des pertes de paquets dans le réseau, et la détection d'intrusion dans le réseau.

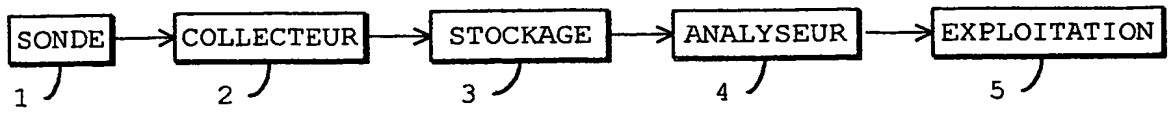


FIG. 1

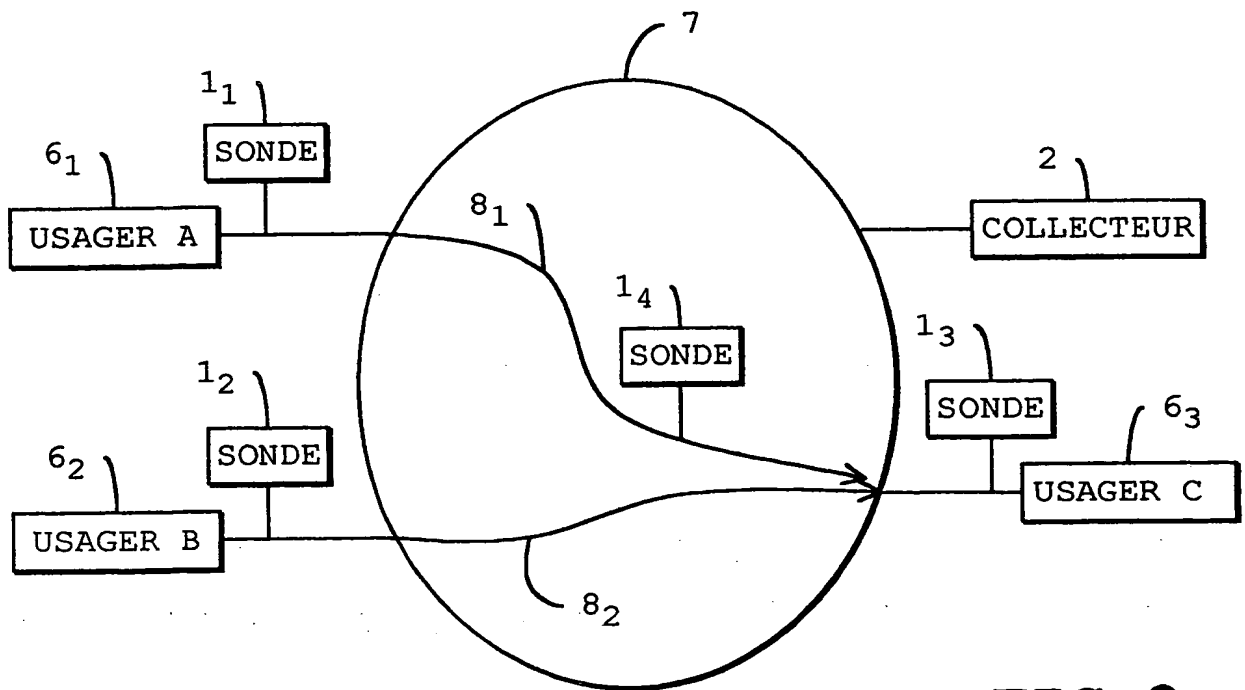


FIG. 2

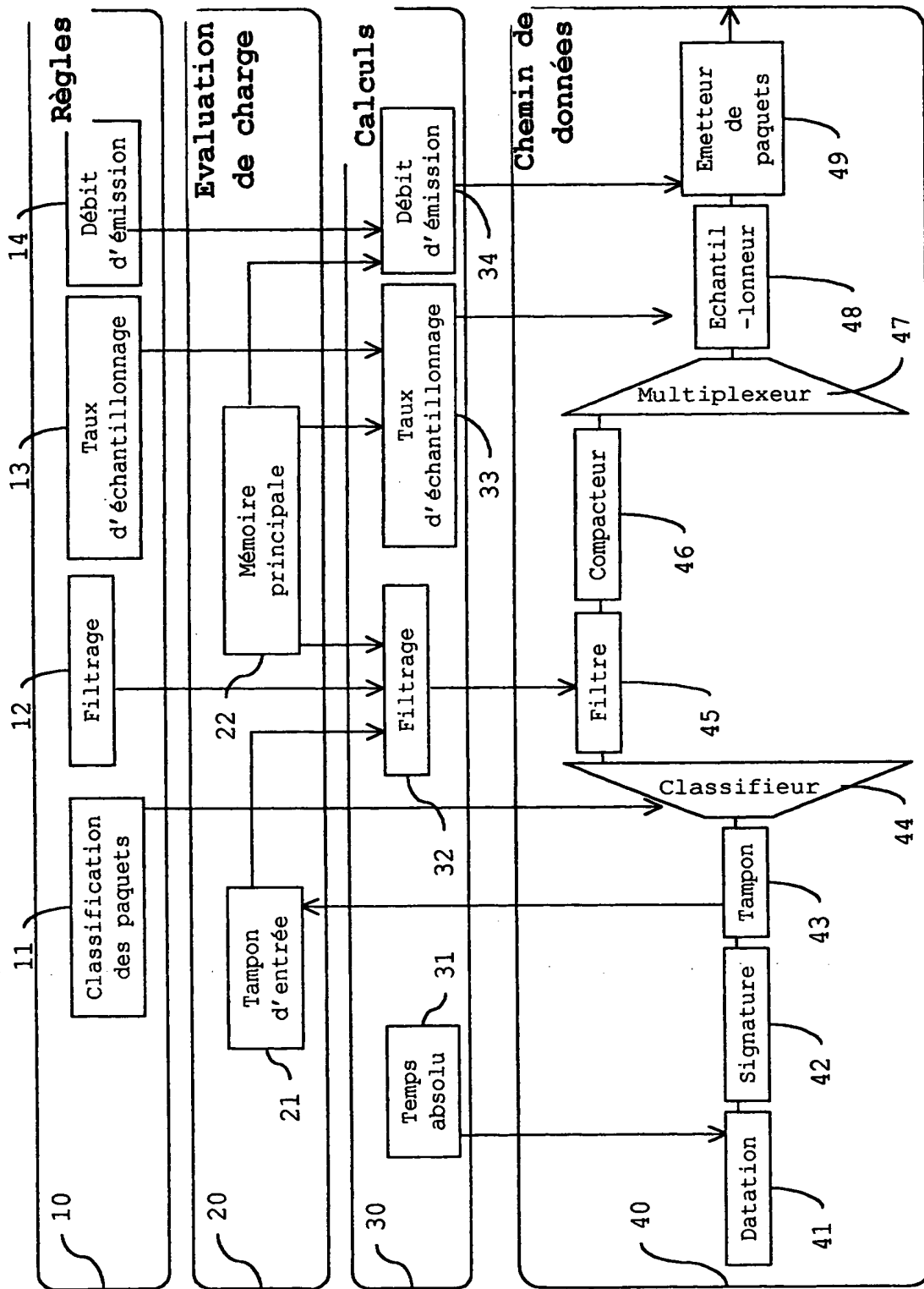


FIG. 3